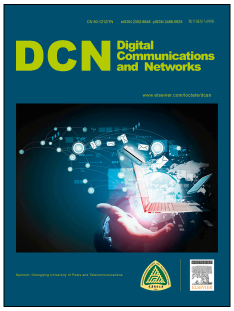

A Distributed Authentication and Authorization Scheme for In-Network Big Data Sharing

Ruidong Li, Hitoshi Asaeda, Jie Li, Xiaoming Fu

PII: S2352-8648(17)30067-6

DOI: 10.1016/j.dcan.2017.06.001

Reference: DCAN 86

To appear in: *Digital Communications and Networks*

Received Date: 15 February 2017

Revised Date: 12 June 2017

Accepted Date: 13 June 2017

Please cite this article as: R. Li, H. Asaeda, J. Li, X. Fu, A Distributed Authentication and Authorization Scheme for In-Network Big Data Sharing, *Digital Communications and Networks* (2017), doi: 10.1016/j.dcan.2017.06.001.

Digital Communications and Networks(DCN)

HOSTED BY
ELSEVIER

Available online at www.sciencedirect.com
ScienceDirect

journal homepage: www.elsevier.com/locate/dcan

A Distributed Authentication and Authorization Scheme for In-Network Big Data Sharing

Ruidong Li*[a], Hitoshi Asaeda[a], Jie Li[b], Xiaoming Fu[c]

[a]**Network System Research Institute, National Institute of Information and Communications Japan (NICT), Tokyo, 184-8795, Japan**
[b]**Department of Computer Science, University of Tsukuba, Ibaraki, 305-8577, Japan**
[c]**Institute of Computer Science, University of Göttingen, Göttingen, 37077, Germany**

Abstract

Big data strongly demands a network infrastructure having the capability to efficiently support data sharing and retrieval. Information-Centric Networking (ICN) approach is an emerging approach to satisfy this demand, where big data is ubiquitously cached in the network and retrieved through names. However, the existing authentication and authorization schemes mostly rely on the centralized servers to provide certificate and mediation services for data retrieval, which causes much traffic overhead for securely sharing data in a distributed manner. To solve this problem, we employ the Identity-Based Cryptography (IBC) to propose a distributed authentication and authorization scheme (DAAS), where the Identity-Based Signature (IBS) is used to achieve distributed verifications on the identities of Publishers and Users and the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is used to enable the distributed and fine-grained authorization. DAAS consists of three phases, initialization, secure data publication, and secure data retrieval, which seamlessly integrate authentication and authorization with the Interest/Data communication paradigm in ICN. In particular, we propose trustworthy registration and Network Operator and Authority Manifest (NOAM) dissemination to provide initial secure registration and enable efficient authentication for global data retrieval. Meanwhile, Attribute Manifest (AM) distribution coupling with automatic attribute update is proposed to reduce the cost for attribute retrieval. We examine the performance of the proposed DAAS, which shows that it can achieve lower bandwidth cost compared to the existing schemes.

KEYWORDS:
Big data, security, authentication, access control, in-network data sharing, information-centric network

1. Introduction

Billions of people with mobile devices and small things, such as sensors, actuators, and robots, are generating tremendous amounts of data [1]. It is known as big data, characterized by five aspects as volume, variety, velocity, value, and complexity [2][3][4]. Big data has attracted wide attentions to develop business applications, including Internet of Things (IoT) services [5] and photo/video sharing [6][7]. It is rapidly increasing as one of the major segments of the today's IT industry.

One of the foundations for big data applications is the data sharing service to efficiently provide data to various entities [7]. Currently, big data sharing services are mostly designed based on Internet technologies, which were originally designed for end-to-end communications. Most of them are implemented based on centralized servers/clouds. Thus, big data is distributed from the distant server/cloud to Users possibly through the similar paths. Because of these, the current big data sharing applications bring out large redundant and duplicate traffic as well as large latency.

Take a big data provision service platform for ex-

*Ruidong Li (Corresponding author) is the corresponding author with the Network System Research Institute, National Institute of Information and Communications Technology, 184-8795, Japan (email: lrd@nict.go.jp).